Information Systems and Security Policy

(*Approved November 22, 2017*; *replaces the* Acceptable Use Policy for Computer and Internet Use *and the* Electronic Communications Equipment Policy.)

I. Intent:

The purpose of the Information Systems and Security Policy is to protect the judicial branch's information technology (IT) resources and to allow for current and future oversight of IT resources, restricting access as needed for security while still promoting the daily ability to conduct business and provide services.

II. Applicability:

This Information Systems and Security Policy shall apply to all judicial officers and employees of the Nebraska Supreme Court (NSC). Where indicated, this policy shall also apply to contract workers and internship positions. Any judicial officer, employee, intern or contractor (end user) of the judicial branch is also governed by NITC (Nebraska Information Technology Commission) standards, when not in conflict with internal judicial branch policies.

III. Acceptable Use:

Use of judicial branch equipment and networks shall be prioritized for professional communications and handling of work-related business. Employees can use the equipment for personal use "within reasonable limits," which means it cannot result in loss of work productivity, interfere with official duties or result in additional expense. End users should not have any expectations of privacy regarding personal business conducted on equipment or networks provided through the judicial branch unless protected by state or federal law. All use is subject to applicable state and federal laws and regulations, such as public record laws of the State of Nebraska as well as Supreme Court rules. Routine monitoring of individual end users will not occur however NSC-IT will perform some routine monitoring of overall use of equipment or networks. In the event of reported or suspected violation of this policy, the State Court Administrator, the State Probation Administrator, or their designee may authorize monitoring of usage by a person subject to this policy, including Internet access and e-mail transmission, to be conducted by State of Nebraska Office of the Chief Information Officer (OCIO) or an applicable service provider. Unacceptable uses of judicial branch equipment and networks include, but are not limited to, violation of the privacy of other users and their data; malicious or disruptive use; unsolicited advertising, fund-raising or other for-profit activities;

misrepresentation of the judicial branch; and use of unauthorized software or hardware in violation of license agreements. See also: NITC 7-101: Acceptable Use Policy State Data Communication Network.

IV. Access Control:

a. Physical Access

i. The data center shall only be accessible by the Network Administrator. If a contract worker or anyone else needs to access NSC's servers in the data center the Network Administrator must accompany them. Physical access to the data center shall be granted by smart card credentials and fingerprint scanning of the Network Administrator by the OCIO and building security.

ii. Access to the storage vault(s) used for equipment storage by the NSC-IT (Nebraska Supreme Court Information Technology) Department in the basement of the state Capitol shall be controlled by the Court Administrator's office. The employee (employee, intern or contractor) must have smart card access to the basement of the Capitol and a vault key, or be accompanied by an authorized employee.

iii. Access to the NSC-IT work areas will be secured to ensure the protection of stored computer assets, as well as preventing unauthorized access to any IT workstations and equipment.

iv. NSC-IT will have a smart card and / or key access to all employee work areas before, during and after work hours for emergency IT purposes. NSC-IT will schedule visits ahead of time wherever possible.

v. Devices are available for checkout that allow end users to utilize hardware or software needed to do their job while away from their office. NSC-IT will manage access to and security for these devices. End users are responsible for safekeeping during the period in which they are checked out.

vi. Use of removable media shall be limited to purposes of direct support of work-related functions where other means of secure data transfer are not available. Only removable media issued by NSC-IT shall be used on judicial branch owned or leased equipment. NSC-IT will be responsible for scanning and securing removable media when not in use.

b. User Access

i. The Network Administrator and or NSC-IT is responsible for creating user accounts and accompanying passwords, active directory (AD) structures for different departments and the needed group policies (GPO) to accompany them within the NSCAP (Nebraska Supreme Court Administration and Probation) domain. The state OCIO is responsible for exchange services and all other services and applications it provides and administers support for.

ii. When an employee position is open for hire, the hiring manager must notify the Network Administrator as soon as possible by submitting the approved NSC-IT checklist. This is necessary in order to facilitate procuring the hardware by the employee's start date.

iii. Once an employee has passed a background check and has been formally hired, the manager must then notify NSC-IT by submitting the approved form. Depending upon the needs of the position and requirements of the hiring manager, the new employee will be given access to the NSCAP domain. This will facilitate the creation of AD accounts, creation of a state email account and forwarding of the new employee's information on to other departments for additional program accounts to be created. Employees may be issued state equipment for accessing state systems. Employees will also be given access needed for web applications and necessary software relating to the position.

iv. State issued cellular devices are available upon the approval of the hiring manager assuming the position is eligible for a cellular device. The phone must be requested through the Network Administrator or other designated Communications Coordinators authorized to procure through the OCIO.

v. Personal phones may have state email accounts installed on them but only after the required form is filled out and returned to the Network Administrator, signed by the Court Administrator and Chief Information Officer for the state. See: NITC 5-204: Linking a Personal Portable Computing Device to the State Email System.

vi. Hiring managers must notify the NSC-IT department of any upcoming employee termination/separation. For security reasons, all accounts must be immediately disabled upon any employee leaving his or her position. Any data that is still needed, whether email or network-related, must be transferred or saved by 5 p.m. on the employee's last day. For unplanned separations, the hiring manager must contact NSC-IT immediately.

vii. Contractors / Interns

Access for contractors or interns must be requested by the administrator or director of the department under which the systems reside. An AD account and a state email account can be created by NSC-IT at the request of the administrator or director.

c. Network Access

i. The Network Administrator is responsible for the NSCAP domain and all servers running within that domain. The Administrator is responsible for the daily upkeep, setup, disaster recovery and usage of these servers. The Administrator must be a part of any planned changes to the NSCAP domain, or usage of the domain by employees or third parties.

ii. The Network Administrator shall be the only one who is allowed to make programmatic changes to the NSCAP servers unless designated otherwise by the Administrator. The NSC-IT department is allowed to access AD for user setup and disabling user accounts along with creating file server shares. The NSC-IT department is also allowed to push software installs and updates over the NSCAP domain to its employees as needed.

iii. The Network Administrator shall utilize AD security event logs to log login and logout times for NSCAP domain access. The Network Administrator will also be responsible for administering the judicial branch's Mobile Device Management (MDM) solution for all state

purchased mobile devices.

iv. The state OCIO department is responsible for VPN creation, upkeep and usage monitoring for all judicial branch employees, contractors and interns.

d. Computer Access

i. Only NSC devices with NSCAP user accounts shall be allowed to log onto the NSCAP domain. No other devices will have access to shared drives or applications residing on the NSCAP domain or VPN access to the NSCAP domain.

ii. User accounts will use ID's of employees' first initial of their first name and their whole last name. If this user ID is already taken, a middle initial will be used after the first initial of the first name. The password will conform to minimum password requirements. See NITC 8-302 Minimum Password Configuration. NSC-IT will not override these requirements for any employee.

iii. All judicial branch employees with system administrative credentials and contractors must use the state's VPN solution with dual authentication.

e. Application Access

i. All computers assigned from the NSC-IT department will have an operating system and basic software package that will allow employees to perform all necessary job responsibilities. Each office shall have software to fit their specific needs.

ii. If the application is controlled by the NSC-IT department, they will furnish the username and password and be in charge of resetting passwords. If the application is controlled by the individual departments, that department must appoint a person to handle usernames and passwords.

iii. Terminated end users must have their application access removed within 3 calendar days by the responsible department.

V. Procurement:

a. The State Court Administrator, the State Probation Administrator or his or her designee, has the authority to approve contracts for the purchase or lease of electronic communications devices, and the accompanying services under which the Administrative Office of the Courts and Probation is the official "customer" to be billed. All purchases/leases of this type of equipment/services will be made through NSC-IT or the OCIO.

b. The judicial branch may provide employees with computer equipment and appropriate licensed software for business use. The hiring manager is responsible for ensuring that purchase of any software and/or hardware for use by an employee conforms to the needs of the position. Hiring managers must follow procedures for requesting hardware/software through NSC-IT. Technology provided by the judicial branch for use in county courthouses will follow a set of published standards.

c. The judicial branch may provide employees with mobile devices with a data plan for use in conducting official business outside the workplace when there is a significant business-related reason for doing so. Hiring managers must follow procedures for requesting mobile devices through NSC-IT.

d. The judicial branch will only procure electronic payment services, either online or point-of-sale, that have been approved through the State of Nebraska's contract process. These contracts shall ensure that the provider is fully PCI-DSS compliant and is subject to annual reviews of compliance status.

e. It is best practice when dealing with IT services to negotiate a Service Level Agreement (SLA). Be sure to keep the following points in mind when negotiating the SLA. Have the SLA reviewed by our legal counsel.

i. Full description of all services provided

ii. Responsibilities of all parties involved

iii. Ownership of data / programing code

iv. Uptime requirements

VI. Data Protection and Destruction:

a. Network drive storage is provided for court employees with backup protection and disaster recovery for work-related data storage.

b. All data created and or stored on state networks, computers, peripherals or otherwise is property of the Supreme Court.

c. Any confidential or restricted data saved to the file server needs to be made a part of a data inventory maintained by NSC-IT. Examples include Social Security numbers, individual health information, financial information, et cetera. See NITC 8-902 Data Classification Categories.

d. Restricted and confidential data should not be transferred unless encrypted.

e. Data that is past its retention period or that is no longer used or needed should be deleted in a timely manner. Hiring managers must inform NSC-IT upon an employee's separation from the judicial branch on whether local data, emails, and network data can be purged, or must be saved to another location.

f. As physical data storage media such as hard drives, thumb drives, DVD's / CD's, et cetera, wear out, they must be physically destroyed by NSC-IT.

VII. Employee Responsibilities:

a. It is the responsibility of all employees to follow the Information Systems and Security Policy. All judicial branch employees must also review IT security training materials each year to maintain compliance.

b. All employees are responsible for being security minded when dealing with passwords, hardware and state data. Passwords shall not be written down. Encrypted password keepers and training on how to use them can be provided by NSC-IT.

c. Employees should only login with their own credentials to any network or application. Sharing of login credentials is not allowed.

d. When an employee leaves his or her desk or computer, the employee will lock the device (Win+L).

e. An employee who is assigned technology equipment is responsible for safeguarding the equipment and controlling its use. Any employee whose equipment is mislaid or stolen should immediately report the loss or theft of such equipment to his or her supervisor and to the NSC-IT for proper incident reporting. If loss or damage of judicial branch owned equipment was caused by negligence on the part of the employee, the cost to replace or repair the item may be passed on to the employee. Upon separation from judicial branch employment, the employee is required to release any assigned equipment back to hiring manager or supervisor.

f. An employee who detects malware or any other compromise of the employee's device should immediately make a report to NSC-IT for proper incident reporting.

g. Employees will ensure that all removable media checked out to them will be secured at all times. Once an item of removable media has been used on a device not owned or leased by the judicial branch, it must be returned to NSC-IT for security scanning. Loss or theft of any item of removable media must be reported immediately to an employee's supervisor and NSC-IT.

h. Employees/contractors must utilize VPN whenever they are not directly connected to the state network. VPN must be used on any unsecured or public connection.

i. All judicial branch employees using state issued mobile devices must password protect the devices with a minimum of a 4-digit pin number. Stronger types of access control such as a longer password, thumbprint recognition are also acceptable. Personal mobile devices used to access state email must also adhere to the above guidelines.

VIII. Remedial Action:

Remedial action for a violation of this policy may include disciplinary proceedings against the individual or individuals responsible, including termination of employment or reporting to the appropriate disciplinary authority. Criminal activity performed using any judicial branch device or system can result in criminal investigation and/or prosecution.